8

Administración de la Seguridad del Usuario

Objetivos

Al finalizar esta lección, debería estar capacitado para:

- Crear y gestionar cuentas de usuario de base de datos:
  - Autenticar usuarios
  - Asignar áreas de almacenamiento por defecto (tablespaces)
- Otorgar y revocar privilegios
- Crear y gestionar roles
- Crear y gestionar perfiles:
  - Implantar funciones estándar de seguridad con contraseña
  - Controlar el uso de recursos por los usuarios

Objetivos

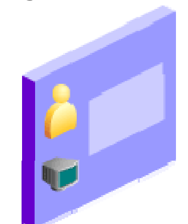
Los siguientes términos están relacionados con la administración de usuarios de base de datos y le ayudarán a comprender los objetivos:

- Una *cuenta de usuario de base de datos* es un medio de organizar la propiedad y el acceso a objetos de base de datos.
- Una *contraseña* es una autenticación por parte de Oracle Database.
- Un *privilegio* es un derecho para ejecutar un tipo concreto de sentencia SQL o para acceder a un objeto de otro usuario.
- Un *rol* es un grupo con nombre de privilegios relacionados que se otorgan a los usuarios o a otros roles.
- Los *perfiles* imponen un juego con nombre de límites de recursos en cuanto al uso de la base de datos y de los recursos de la instancia y, además, gestionan el estado de las cuentas y las reglas de gestión de las contraseñas.
- La *cuota* es un espacio asignado en un tablespace determinado. Es uno de los métodos mediante los que puede controlar el uso de recursos por parte de los usuarios.

Cuentas de Usuario de Base de Datos

Cada cuenta de usuario de base de datos tiene lo siguiente:

- Nombre de usuario único
- Método de autenticación
- Tablespace por defecto
- Tablespace temporal
- Perfil de usuario
- Grupo de consumidores inicial
- Estado de cuenta



Un esquema:

- Es una recopilación de objetos de base de datos propiedad de un usuario de la base de datos
- Posee el mismo nombre que la cuenta de usuario

ORACLE

Cuentas de Usuario de Base de Datos

Para acceder a la base de datos, un usuario debe especificar una cuenta de usuario de base de datos válida y autenticarse correctamente según los requisitos de dicha cuenta de usuario. Cada usuario de base de datos tiene una cuenta de base de datos única.

Oracle recomienda esto para evitar posibles agujeros en la seguridad y proporcionar datos significativos para ciertas actividades de auditoría. Sin embargo, los usuarios comparten a veces una cuenta de base de datos común. En estos raros casos, el sistema operativo y las aplicaciones deben proporcionar la seguridad adecuada para la base de datos. Cada cuenta de usuario tiene lo siguiente:

- **Nombre de usuario único:** los nombres de usuario no pueden superar los 30 bytes ni contener caracteres especiales y deben empezar por una letra.
- **Método de autenticación:** el método de autenticación más común es una contraseña, pero Oracle Database 11*g* soporta los métodos de autenticación por contraseña, global y externa (como la autenticación biométrica, mediante certificado y mediante token).
- **Tablespace por defecto:** éste es el lugar en el que el usuario creará objetos si no especifica ningún otro tablespace. Tenga en cuenta que disponer de un tablespace por defecto no implica que el usuario tenga el *privilegio* de crear objetos en dicho tablespace, ni tampoco que tenga una *cuota* de espacio en dicho tablespace en la que crear objetos. Ambos se otorgan por separado.

Cuentas de Usuario de Base de Datos (continuación)

- **Tablespace temporal:** es un lugar en el que la instancia crea objetos temporales como, por ejemplo, ordenaciones y tablas temporales en nombre del usuario. No se aplica ninguna cuota a los tablespaces temporales.
- **Perfil de usuario:** es un juego de restricciones de recurso y contraseña asignadas al usuario.
- **Grupo de consumidores inicial:** es una opción utilizada por el gestor de recursos.
- **Estado de cuenta:** los usuarios sólo pueden acceder a las cuentas "abiertas". `account_status` puede tener diversas combinaciones de "bloqueada" y "caducada".

Esquemas: un *esquema* es una recopilación de objetos de base de datos propiedad de un usuario de la base de datos. Los objetos de esquema son estructuras lógicas que hacen referencia directa a datos de la base de datos. Los objetos de esquema incluyen estructuras como, por ejemplo, tablas, vistas, secuencias, procedimientos almacenados, sinónimos, índices, clusters y enlaces de base de datos. En general, los objetos de esquema incluyen todo lo que la aplicación cree en la base de datos.

Nota: un usuario de base de datos no es necesariamente una persona. Es una práctica habitual crear un usuario que posea los objetos de base de datos de una aplicación en particular, por ejemplo, HR. El usuario de la base de datos puede ser un dispositivo, una aplicación o sólo una manera de agrupar objetos de base de datos por motivos de seguridad. No se necesita la información de identificación personal de una persona para un usuario de la base de datos.

Cuentas Administrativas Predefinidas

- La cuenta SYS:
  - Tiene otorgado el rol DBA, además de otros varios roles
  - Tiene todos los privilegios con ADMIN OPTION
  - Es necesaria para el inicio, el cierre y para algunos comandos de mantenimiento
  - Es propietaria del diccionario de datos y del repositorio de carga de trabajo automática (AWR)
- La cuenta SYSTEM tiene otorgados los roles DBA, MGMT_USER y AQ_ADMINISTRATOR_ROLE.
- La cuenta DBSNMP tiene otorgado el rol OEM_MONITOR.
- La cuenta SYSMAN tiene otorgados los roles MGMT_USER, RESOURCE y SELECT_CATALOG_ROLE.
- Estas cuentas no se utilizan para operaciones rutinarias.

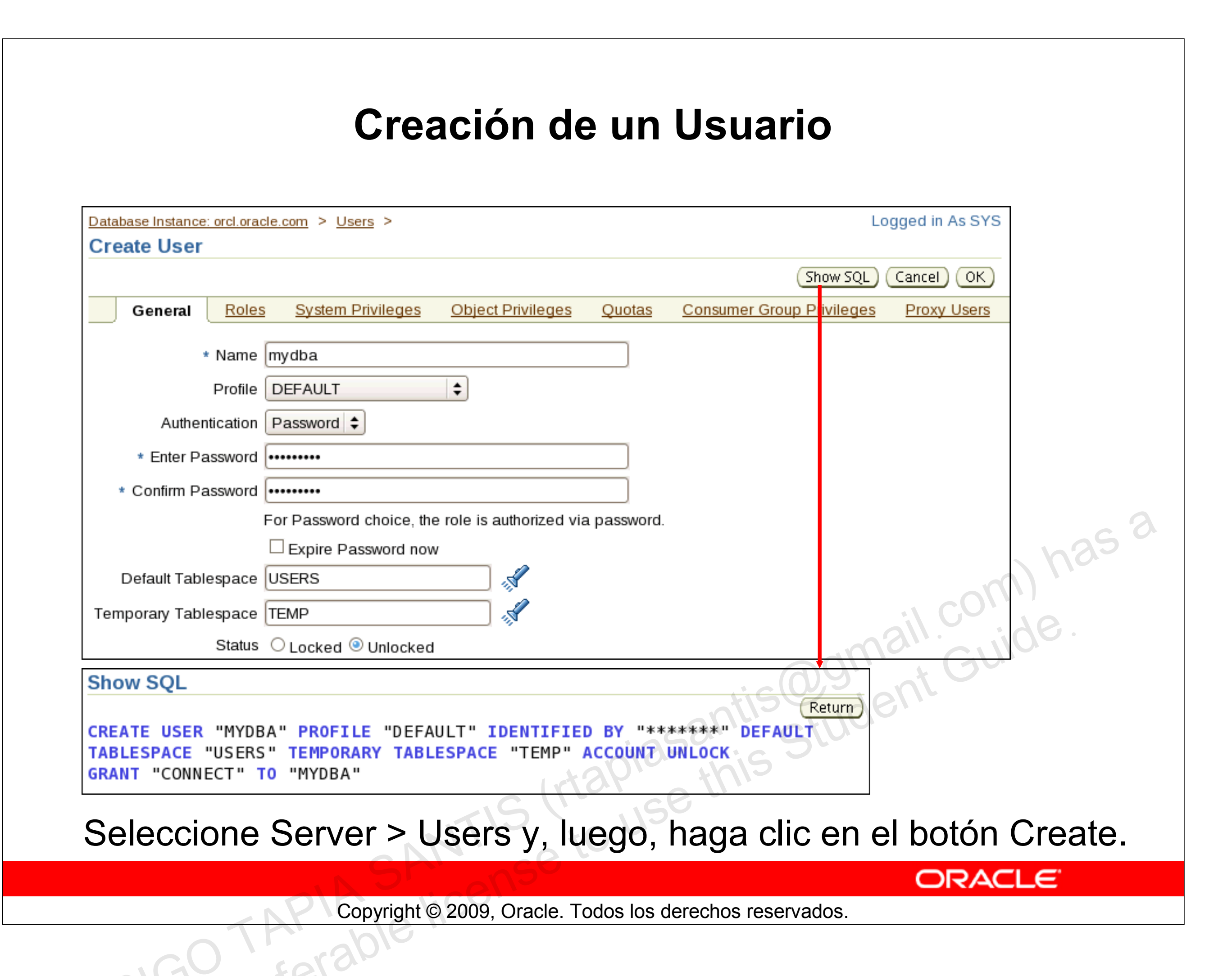
ORACLE

Cuentas Administrativas Predefinidas

Las cuentas SYS y SYSTEM tienen otorgado por defecto el rol de administrador de base de datos (DBA). Además, la cuenta SYS tiene todos los privilegios con la opción ADMIN OPTION y es propietaria del diccionario de datos. Para conectar a la cuenta SYS, debe utilizar la cláusula AS SYSDBA para una instancia de base datos y AS SYSASM para una instancia de la Gestión Automática de Almacenamiento (ASM). Cualquier usuario al que se le otorgue el privilegio SYSDBA puede conectarse a la cuenta SYS mediante la cláusula AS SYSDBA. Sólo los usuarios “con privilegios”, a los que se les otorgan los privilegios SYSDBA, SYSOPER o SYSASM, pueden iniciar y cerrar instancias. La cuenta SYSTEM no tiene el privilegio SYSDBA. SYSTEM también tiene otorgados los roles AQ_ADMINISTRATOR_ROLE y MGMT_USER. Las cuentas SYS y SYSTEM son cuentas necesarias en la base de datos. No se pueden borrar.

El agente de gestión de Enterprise Manager utiliza la cuenta DBSNMP para supervisar y gestionar la base de datos. La cuenta SYSMAN se utiliza para realizar tareas de administración de Oracle Enterprise Manager. Ni DBSNMP ni SYSMAN tienen el privilegio SYSDBA.

Práctica recomendada: debido a la aplicación del principio de privilegio más bajo, estas cuentas no se utilizan para operaciones rutinarias. Los usuarios que necesiten privilegios DBA tienen cuentas separadas a las que se les otorgan los privilegios necesarios. Por ejemplo, Jim tiene una cuenta de privilegio bajo denominada jim y una cuenta con privilegios denominada jim_dba. Este método permite aplicar el principio de privilegio más bajo, elimina la necesidad de compartir cuentas y permite auditar acciones individuales.



Creación de un Usuario

En la página Users de Enterprise Manager, puede gestionar los usuarios de base de datos que pueden acceder a la base de datos actual. Utilice esta página para crear, suprimir y modificar la configuración de un usuario.

Para crear un usuario de base de datos:

1. En Enterprise Manager Database Control, haga clic en el separador Server y, a continuación, haga clic en Users en la sección Security.
2. Haga clic en el botón Create.

Proporcione la información necesaria. Los elementos obligatorios (como Name) aparecen marcados con un asterisco (*). El nombre especificado debe seguir las mismas reglas que las utilizadas para crear los objetos de la base de datos. Las siguientes páginas de esta lección le proporcionan más información sobre la autenticación. Los perfiles se tratarán más adelante en esta lección.

Asigne un tablespace por defecto y un tablespace temporal a cada usuario. Si los usuarios no especifican ningún tablespace al crear un objeto, éste se creará en el tablespace por defecto asignado al propietario del objeto. Esto permite controlar dónde se crean los objetos. Si no selecciona un tablespace por defecto, se utiliza el permanente por defecto definido por el sistema. Es un caso similar al del tablespace temporal: si no especifica ninguno, se utiliza el tablespace temporal definido por el sistema.

Nota: haga clic en Show SQL para ver la sintaxis SQL de soporte. Para ver la sintaxis SQL completa para crear usuarios, consulte el manual *Oracle® Database SQL Language Reference* (Referencia del Lenguaje SQL de Oracle® Database).

Autenticación de Usuarios

- Password
- External
- Global

Edit User: HR

Actions Create Like Go Show SQL Revert Apply

General Roles System Privileges Object Privileges Quotas Consumer Group Privileges Proxy Users

Name HR
Profile DEFAULT
Authentication Password
* Enter Password
* Confirm Password
Password
External
Global
For Password choice, the role is authorized via password.
Expire Password now
Default Tablespace USERS
Temporary Tablespace TEMP
Status Locked Unlocked

ORACLE

Autenticación de Usuarios

La *autenticación* significa verificar la identidad de alguien o algo (un usuario, dispositivo u otra entidad) que desea utilizar datos, recursos o aplicaciones. La validación de dicha identidad establece una relación de confianza para una mayor interacción. La autenticación también permite establecer responsabilidades al posibilitar el enlace de acceso y acciones con identidades concretas. Tras la autenticación, los procesos de autorización pueden permitir o limitar los niveles de acceso y acción permitidos para dicha entidad.

Al crear un usuario, debe decidir la técnica de autenticación que se va a utilizar y que se podrá modificar posteriormente.

Password: también denominada autenticación por Oracle Database. Cree cada usuario con una contraseña asociada que se debe proporcionar cuando el usuario intente establecer una conexión. Al configurar una contraseña, puede establecer que venza inmediatamente, lo que obliga al usuario a cambiar la contraseña después de la primera conexión. Si decide utilizar el vencimiento de contraseñas de usuario, asegúrese de que los usuarios pueden cambiar la contraseña. Algunas aplicaciones no tienen esta función. Todas las contraseñas creadas en Oracle Database 11*g* son sensibles a mayúsculas/minúsculas por defecto. Estas contraseñas también pueden contener caracteres multibyte y están limitadas a 30 bytes. Toda contraseña creada en una base de datos que se actualiza a Oracle Database 11*g* sigue siendo sensible a mayúsculas/minúsculas hasta que se cambie.

Las contraseñas siempre se cifran de forma automática y transparente mediante el algoritmo Advanced Encryption Standard (AES) durante las conexiones de red (cliente/servidor y servidor/servidor) antes de enviarlas por la red.

Autenticación de Usuarios (continuación)

External: se trata de la autenticación con un método ajeno a la base de datos (sistema operativo, Kerberos o Radius). Se necesita Advanced Security Option para Kerberos o Radius. Los usuarios se pueden conectar a la base de datos Oracle sin especificar un nombre de usuario o contraseña. Advanced Security Option (que es una autenticación compleja) permite identificar usuarios mediante biométrica, certificados X509 y dispositivos de token. Con la autenticación externa, la base de datos confía en el sistema operativo subyacente, el servicio de autenticación de red o el servicio de autenticación externa para restringir el acceso a cuentas de base de datos. No se utiliza ninguna contraseña de base de datos para este tipo de conexión. Si el servicio de red o del sistema operativo lo permite, éste podrá autenticar usuarios. Si utiliza la autenticación del sistema operativo, defina el parámetro de inicialización `OS_AUTHENT_PREFIX` y utilice este prefijo en los nombres de usuario Oracle. El parámetro `OS_AUTHENT_PREFIX` define un prefijo que Oracle Database agrega al principio del nombre de cuenta de sistema operativo de cada usuario. El valor por defecto de este parámetro es `OPS$` para la compatibilidad con versiones anteriores del software de Oracle. La base de datos Oracle compara el nombre de usuario con prefijo con los nombres de usuario Oracle de la base de datos cuando un usuario intenta conectarse. Por ejemplo, suponga que `OS_AUTHENT_PREFIX` se ha definido de la siguiente forma:

```
OS_AUTHENT_PREFIX=OPS$
```

Si un usuario con una cuenta de sistema operativo denominada `tsmith` se tiene que conectar a Oracle Database y lo va a autenticar el sistema operativo, Oracle Database comprueba si hay un usuario de base de datos `OPS$tsmith` correspondiente y, si es así, permite al usuario conectarse. Todas las referencias a un usuario autenticado por el sistema operativo deben incluir el prefijo, como se ve en `OPS$tsmith`.

Nota: el texto del parámetro de inicialización `OS_AUTHENT_PREFIX` es sensible a mayúsculas/minúsculas en algunos sistemas operativos. Consulte la documentación de Oracle específica para el sistema operativo si desea más información sobre este parámetro de inicialización.

Global: con Oracle Advanced Security Option, la autenticación global permite identificar usuarios mediante Oracle Internet Directory.

Para obtener más información sobre métodos de autenticación avanzados, consulte el curso *Seguridad de la Base de Datos Oracle*.

Autenticación de Administradores

Seguridad del sistema operativo:

- Los DBA deben tener privilegios del sistema operativo para crear y suprimir archivos.
- Los usuarios típicos de base de datos no deben tener privilegios del sistema operativo para crear o suprimir archivos de base de datos.

Seguridad del administrador:

- Para conexiones de SYSDBA, SYSOPER y SYSASM:
  - Se audita el usuario DBA por nombre para el archivo de contraseñas y los métodos de autenticación compleja
  - Se audita el nombre de la cuenta del sistema operativo para la autenticación del sistema operativo
  - La autenticación del sistema operativo tiene prioridad sobre la autenticación del archivo de contraseñas para los usuarios con privilegios
  - El archivo de contraseñas utiliza contraseñas sensibles a mayúsculas/minúsculas

ORACLE

Autenticación de Administradores

Seguridad del sistema operativo: en UNIX y Linux, por defecto, los DBA pertenecen al grupo del sistema operativo `oinstall`, que posee los privilegios necesarios para crear y suprimir archivos de base de datos.

Seguridad del administrador: las conexiones de los usuarios con privilegios `SYSDBA`, `SYSOPER` y `SYSASM` se autorizan únicamente después de la verificación con el archivo de contraseñas o con los privilegios y los permisos del sistema operativo. Si se utiliza la autenticación del sistema operativo, la base de datos *no* utiliza el nombre de usuario y contraseña proporcionados. La autenticación del sistema operativo se utiliza si no existe archivo de contraseñas, si el nombre de usuario o la contraseña proporcionados no están en ese archivo o si no se proporcionan ningún nombre de usuario y contraseña. El archivo de contraseñas de Oracle Database 11*g* utiliza contraseñas sensibles a mayúsculas/minúsculas por defecto.

No obstante, si la autenticación se produce mediante el archivo de contraseñas, la conexión se registra con el nombre de usuario. Si la autenticación se produce a través del sistema operativo, entonces es una conexión `CONNECT /` que no registra el usuario concreto.

Nota: si es miembro del grupo `OSDBA` u `OSOPER` del sistema operativo y se conecta como `SYSDBA` o `SYSOPER`, lo hará con los privilegios administrativos asociados independientemente del nombre de usuario y contraseña que especifique. Para `SYSASM`, no tiene que especificar ningún nombre de usuario ni ninguna contraseña (por ejemplo, `sqlplus / as SYSASM`).

En Oracle Database 11*g*, el usuario con privilegios puede utilizar métodos de autenticación compleja: Kerberos, SSL o autenticación de directorio si tiene licencia de Advanced Security Option.



Desbloqueo de Cuentas de Usuario y Restablecimiento de Contraseñas

Durante la instalación y la creación de la base de datos, puede desbloquear y restablecer muchas de las cuentas de usuario de base de datos proporcionadas por Oracle. Si no ha seleccionado desbloquear las cuentas de usuario en ese momento, puede desbloquear un usuario si lo selecciona en la página Users, selecciona Unlock User en la lista Actions y hace clic en Go. Esto no cambia la contraseña de ninguna manera. Si la contraseña está caducada en el momento en que desbloquea el usuario, permanecerá caducada hasta que edite el usuario y cambie la contraseña.

Para desbloquear el usuario y restablecer la contraseña, realice los siguientes pasos en la página Edit Users:

1. Introduzca la nueva contraseña en los campos Enter Password y Confirm Password.
2. Active la casilla de control Unlocked.
3. Haga clic en Apply para restablecer la contraseña y desbloquear la cuenta de usuario.

Privilegios

Hay dos tipos de privilegios de usuario:

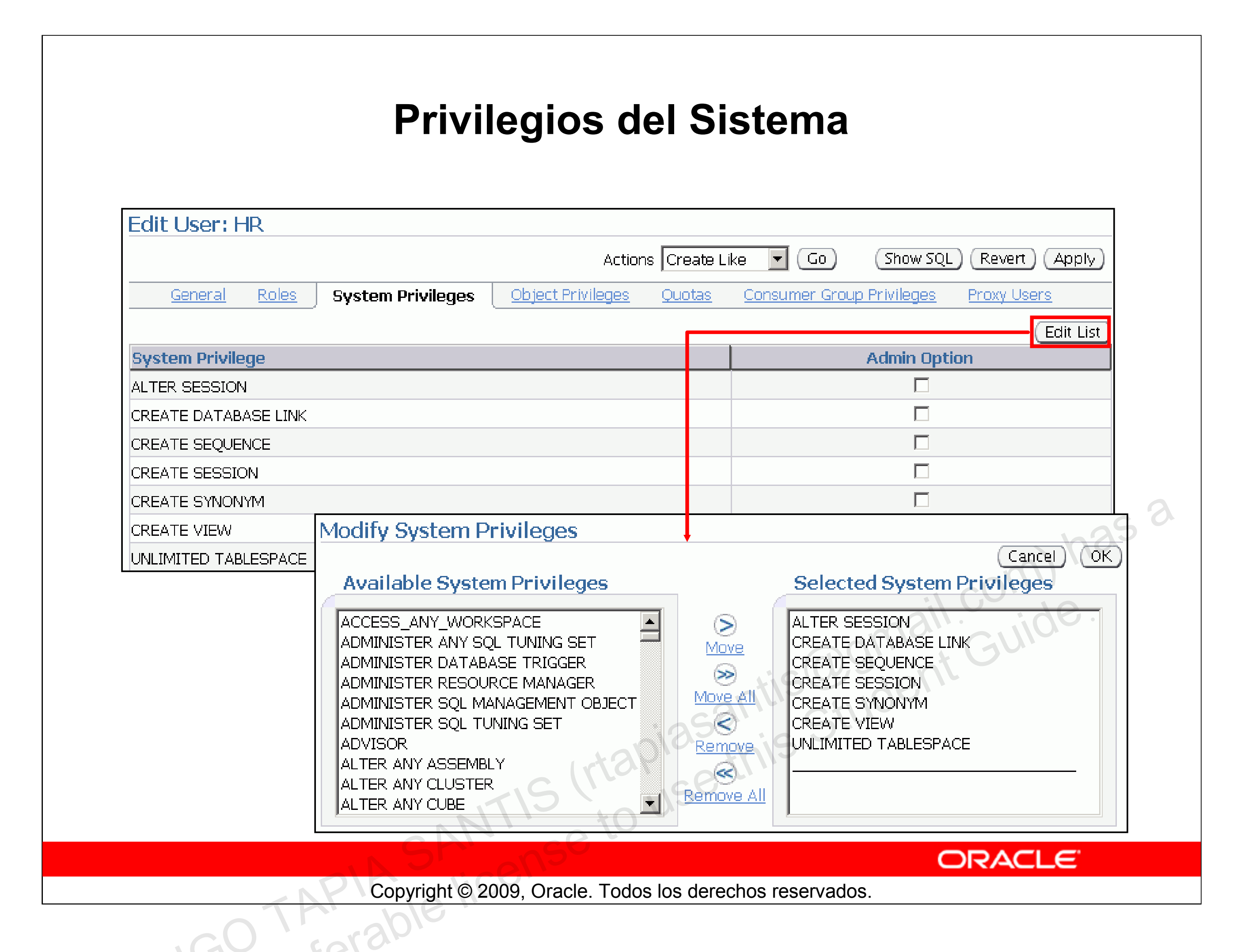
- Sistema: permite a los usuarios realizar acciones concretas en la base de datos
- Objeto: permite a los usuarios acceder y manipular un objeto concreto

Privilegios

Un *privilegio* es un derecho para ejecutar un tipo concreto de sentencia SQL o para acceder a un objeto de otro usuario. Oracle Database le permite controlar lo que los usuarios pueden o no pueden hacer en la base de datos.

Los privilegios se dividen en dos categorías:

- **Privilegios del sistema:** cada privilegio del sistema permite a un usuario realizar una operación de base de datos concreta o una clase de operaciones de base de datos. Por ejemplo, el privilegio para crear tablespaces es un privilegio del sistema. Estos privilegios los puede otorgar el administrador o alguien a quien se le haya proporcionado explícitamente permiso para administrar el privilegio. Existen más de 170 privilegios del sistema distintos. Muchos de ellos contienen la cláusula `ANY`.
- **Privilegios de objeto:** los privilegios de objeto permiten a un usuario realizar una acción concreta en un objeto determinado, como una tabla, una vista, una secuencia, un procedimiento, una función o un paquete. Sin el permiso concreto, los usuarios sólo pueden acceder a sus propios objetos. Estos privilegios los puede otorgar el propietario de un objeto, el administrador o alguien al que se le haya proporcionado explícitamente permiso para otorgar privilegios sobre el objeto.



Privilegios del Sistema

Para otorgar privilegios del sistema, haga clic en el separador Systems Privileges de la página Edit User. Seleccione los privilegios adecuados de la lista de privilegios disponibles y muévalos a la lista Selected System Privileges haciendo clic en la flecha Move.

Otorgar un privilegio con la cláusula `ANY` significa que el privilegio traspasa las líneas del esquema. Por ejemplo, si tiene el privilegio `CREATE TABLE`, puede crear una tabla, pero sólo en su propio esquema. El privilegio `SELECT ANY TABLE` le permite realizar selecciones en tablas propiedad de otros usuarios. El usuario `SYS` y los usuarios con el rol `DBA` tienen otorgados todos los privilegios `ANY`; por lo tanto, pueden realizar cualquier acción en cualquier objeto de datos. El ámbito de los privilegios del sistema `ANY` se puede controlar con la opción de Oracle Database Vault.

Si se activa la casilla de control Admin Option, el usuario podrá administrar el privilegio del sistema y otorgarlo a otros usuarios.

La sintaxis SQL para otorgar privilegios del sistema es la siguiente:

```
GRANT <system_privilege> TO <grantee clause> [WITH ADMIN OPTION]
```

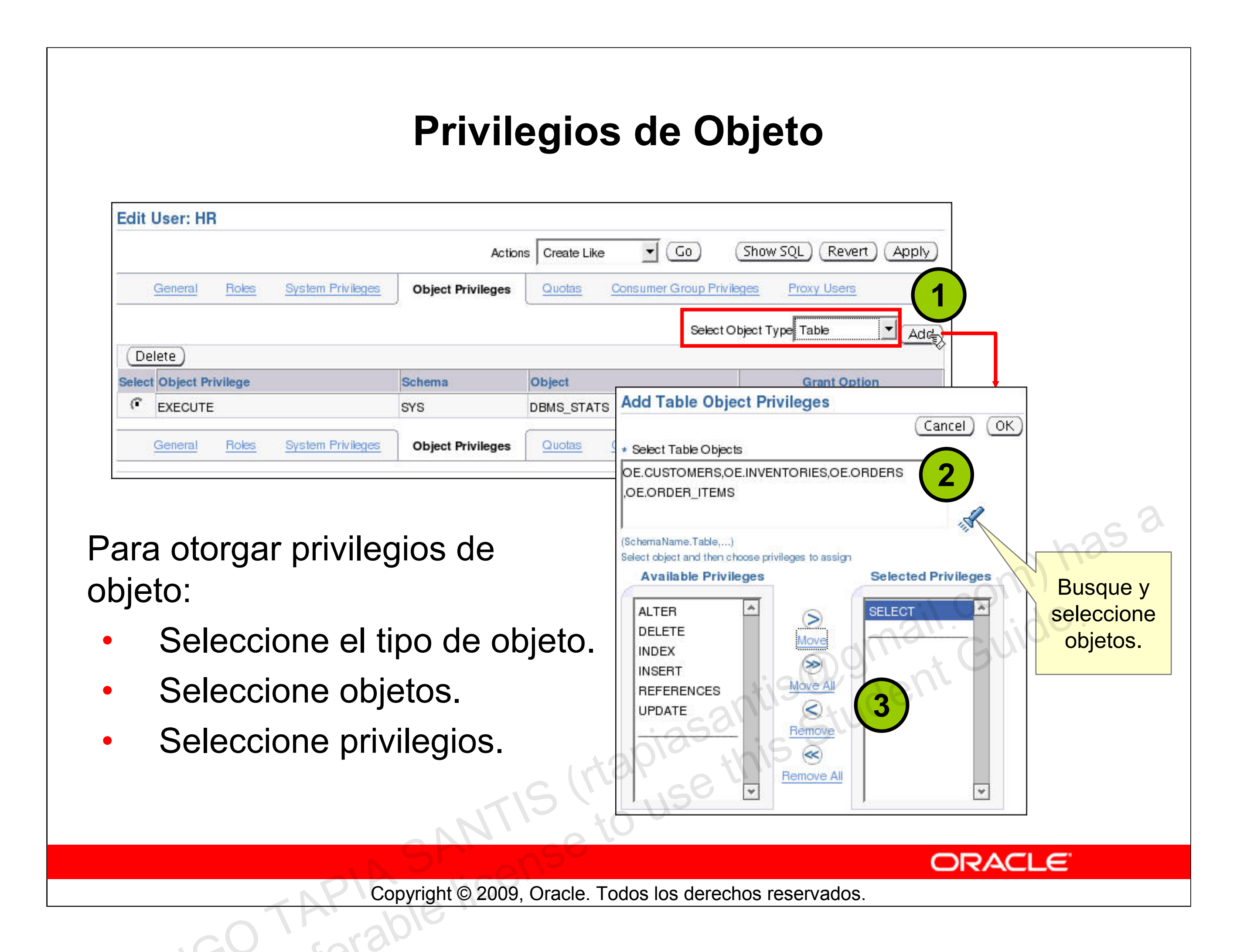
Considere detenidamente los requisitos de seguridad antes de otorgar permisos del sistema. Algunos privilegios del sistema se suelen otorgar sólo a los administradores:

- **`RESTRICTED SESSION`:** este privilegio le permite conectarse incluso aunque la base de datos se haya abierto en modo restringido.

Privilegios del Sistema (continuación)

- **SYSDBA y SYSOPER:** estos privilegios le permiten cerrar, iniciar y realizar una operación de recuperación y demás tareas administrativas en la base de datos. SYSOPER permite a un usuario realizar tareas operativas básicas, pero sin la capacidad de ver los datos de usuarios. Incluye los siguientes privilegios del sistema:
  - STARTUP y SHUTDOWN
  - CREATE SPFILE
  - ALTER DATABASE OPEN/MOUNT/BACKUP
  - ALTER DATABASE ARCHIVELOG
  - ALTER DATABASE RECOVER (Sólo recuperación completa. Cualquier tipo de recuperación incompleta, como UNTIL TIME|CHANGE|CANCEL|CONTROLFILE, necesita una conexión como SYSDBA.)
  - RESTRICTED SESSION

  El privilegio del sistema SYSDBA autoriza además la recuperación incompleta y la supresión de una base de datos. De hecho, el privilegio del sistema SYSDBA permite a un usuario conectarse como usuario SYS.
- **SYSASM:** este privilegio le permite iniciar, cerrar y administrar una instancia de ASM.
- **DROP ANY *objeto*:** el privilegio DROP ANY le permite suprimir objetos propiedad de otros usuarios de esquema.
- **CREATE, MANAGE, DROP y ALTER TABLESPACE:** estos privilegios permiten la administración de tablespaces, incluida la creación, el borrado y el cambio de sus atributos.
- **CREATE LIBRARY:** Oracle Database permite a los desarrolladores crear y llamar a código externo (por ejemplo, una biblioteca C) desde PL/SQL. La biblioteca debe recibir el nombre de un objeto LIBRARY de la base de datos. El privilegio CREATE LIBRARY permite al usuario crear una biblioteca de código arbitrario ejecutable desde PL/SQL.
- **CREATE ANY DIRECTORY:** como medida de seguridad, el directorio del sistema operativo en el que reside el código debe estar enlazado a un objeto de directorio Oracle virtual. Con el privilegio CREATE ANY DIRECTORY, podría llamar a objetos de código no seguros. El privilegio CREATE ANY DIRECTORY permite a un usuario crear un objeto de directorio (con acceso de lectura y escritura) en cualquier directorio al que el propietario del software de Oracle pueda acceder. Esto significa que el usuario puede acceder a procedimientos externos en esos directorios. El usuario puede intentar leer y escribir cada archivo de base de datos directamente, ya sean archivos de datos, redo logs y logs de auditoría. Asegúrese de que su organización posee una estrategia de seguridad que evita que se haga un uso incorrecto de privilegios potentes como éste.
- **GRANT ANY OBJECT PRIVILEGE:** este privilegio le permite otorgar permisos sobre objetos que no le pertenecen.
- **ALTER DATABASE y ALTER SYSTEM:** estos privilegios son muy potentes y le permiten modificar la base de datos y la instancia de Oracle (por ejemplo, cambiar el nombre de un archivo de datos o vaciar la caché de buffers).



Privilegios de Objeto

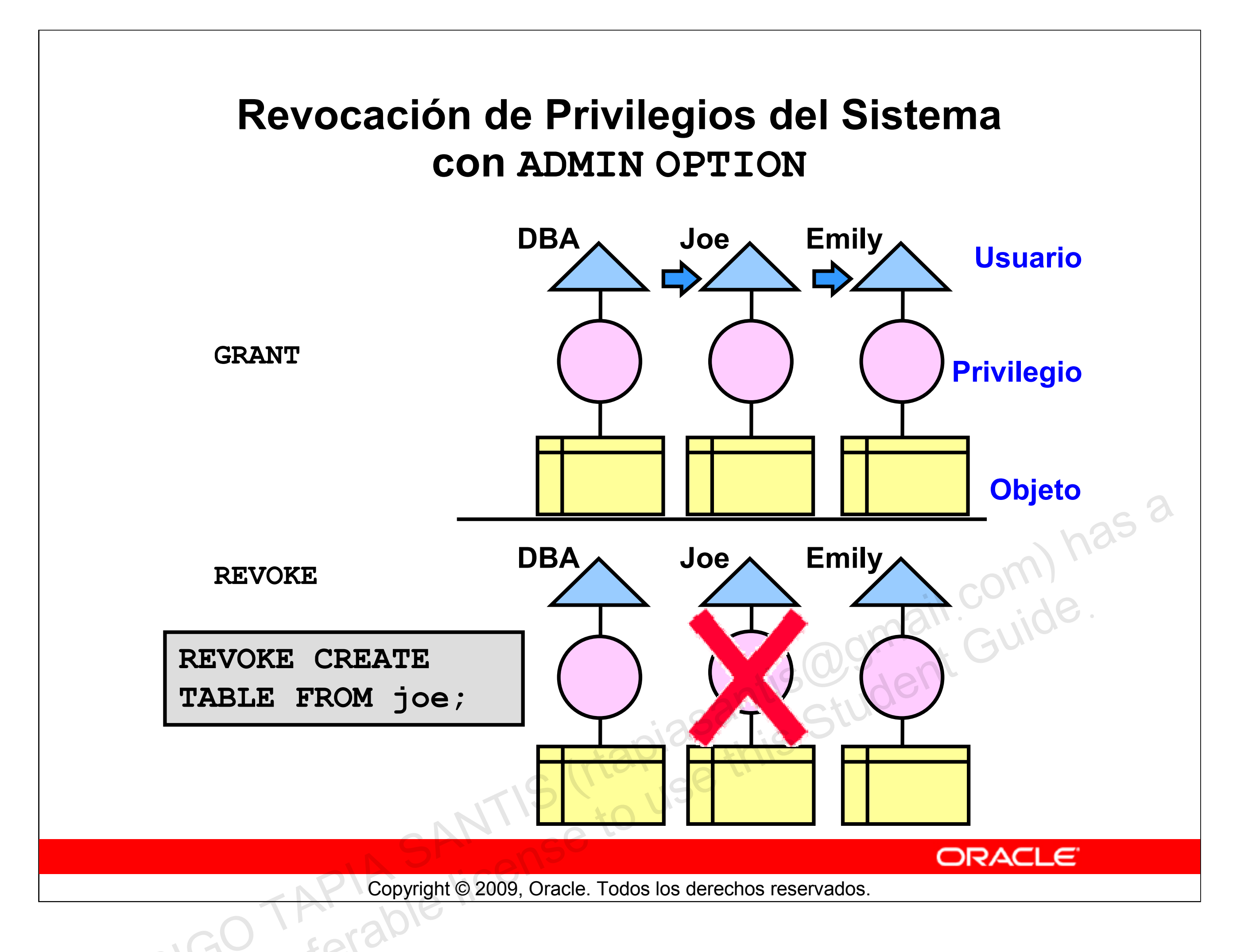
Para otorgar privilegios de objeto, haga clic en el separador Object Privileges de la página Edit User. Seleccione el tipo de objeto para el que desea otorgar los privilegios y, a continuación, haga clic en el botón Add. Para seleccionar los objetos, introduzca <*username.object name*> o selecciónelos en la lista.

A continuación, seleccione los privilegios adecuados de la lista Available Privileges y haga clic en el botón Move. Cuando termine de seleccionar los privilegios, haga clic en OK.

En la página Edit User, active la casilla de control Grant si este usuario puede otorgar el mismo acceso a otros usuarios.

La sintaxis SQL para otorgar privilegios de objeto es la siguiente:

```
GRANT <object_privilege> ON <object> TO <grantee clause>
[WITH GRANT OPTION]
```



Revocación de Privilegios del Sistema con `ADMIN OPTION`

Los privilegios del sistema que se han otorgado directamente con un comando `GRANT` se pueden revocar mediante la sentencia SQL `REVOKE`. Los usuarios con el privilegio del sistema `ADMIN OPTION` pueden revocar el privilegio de cualquier otro usuario de la base de datos. El usuario que lleva a cabo la revocación no tiene que ser el mismo que inicialmente otorgó el privilegio.

No hay ningún efecto en cascada cuando se revoca un privilegio del sistema, independientemente de si se le aplica el privilegio `ADMIN OPTION`.

La sintaxis SQL para revocar privilegios del sistema es la siguiente:

```
REVOKE <system_privilege> FROM <grantee clause>
```

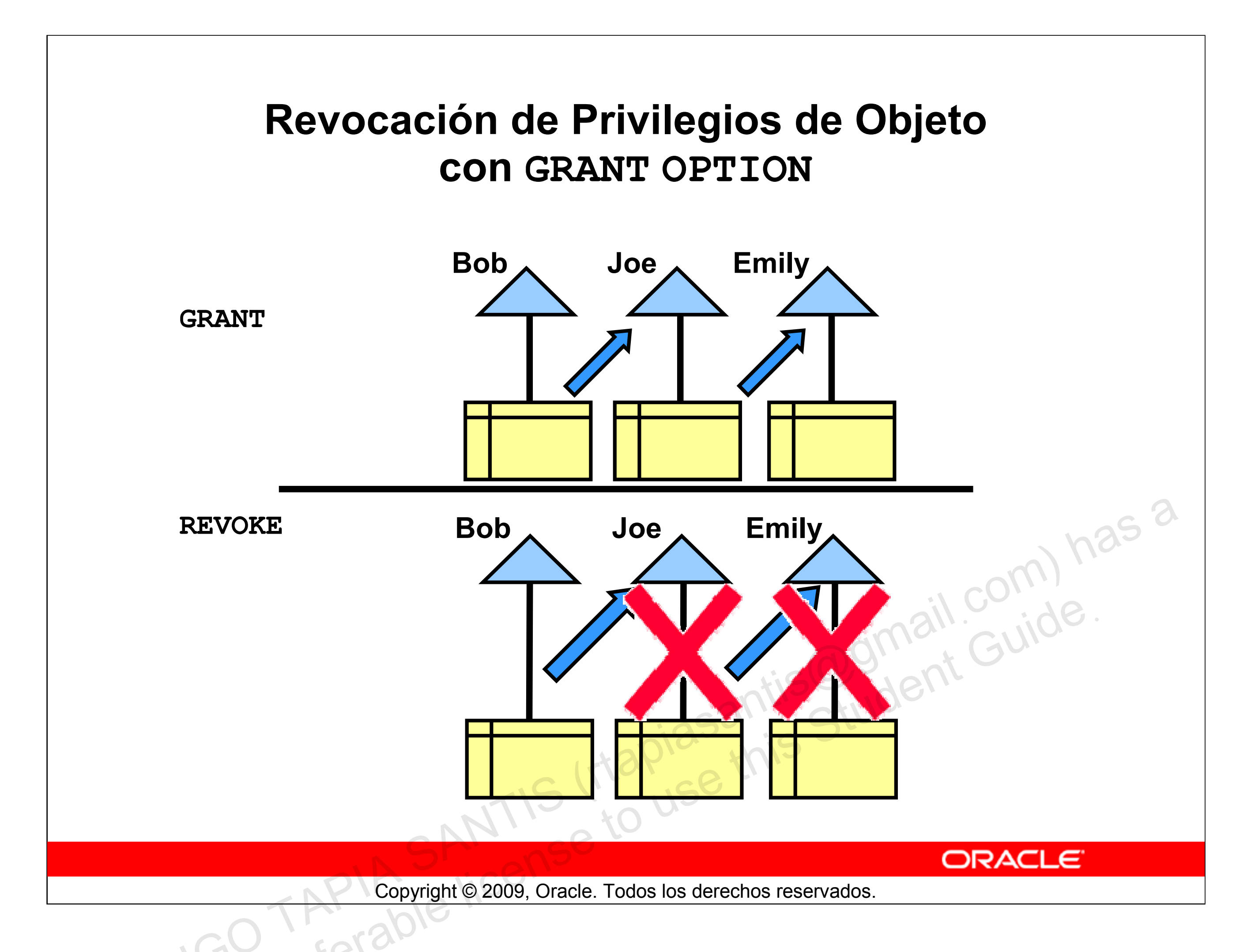
En la diapositiva se ilustra la siguiente situación.

Supuesto

1. El DBA otorga el privilegio del sistema `CREATE TABLE` a Joe con `ADMIN OPTION`.
2. Joe crea una tabla.
3. Joe otorga el privilegio del sistema `CREATE TABLE` a Emily.
4. Emily crea una tabla.
5. El DBA revoca el privilegio del sistema `CREATE TABLE` a Joe.

Resultado

La tabla de Joe aún existe, pero Joe no puede crear nuevas tablas. La tabla de Emily aún existe y todavía posee el privilegio del sistema `CREATE TABLE`.



Revocación de Privilegios de Objeto con `GRANT OPTION`

Se pueden observar efectos en cascada cuando se revoca un privilegio del sistema relacionado con una operación de lenguaje de manipulación de datos (DML). Por ejemplo, si se otorga el privilegio `SELECT ANY TABLE` a un usuario y si ese usuario ha creado procedimientos que utilizan la tabla, todos los procedimientos contenidos en el esquema del usuario se tienen que recompilar antes de que se puedan utilizar de nuevo.

La revocación de privilegios de objeto también produce efectos en cascada mediante `GRANT OPTION`. Como usuario, sólo puede revocar los privilegios que haya otorgado. Por ejemplo, Bob no puede revocar el privilegio de objeto que Joe ha otorgado a Emily. Sólo el usuario con privilegios o un usuario con el privilegio denominado `GRANT ANY OBJECT PRIVILEGE` puede revocar privilegios de objeto.

Supuesto

1. A Joe se le otorga el privilegio de objeto `SELECT` en `EMPLOYEES` con `GRANT OPTION`.
2. Joe otorga el privilegio `SELECT` en `EMPLOYEES` a Emily.
3. A Joe se le revoca el privilegio `SELECT`. Esta revocación tiene un efecto en cascada y se aplica también a Emily.

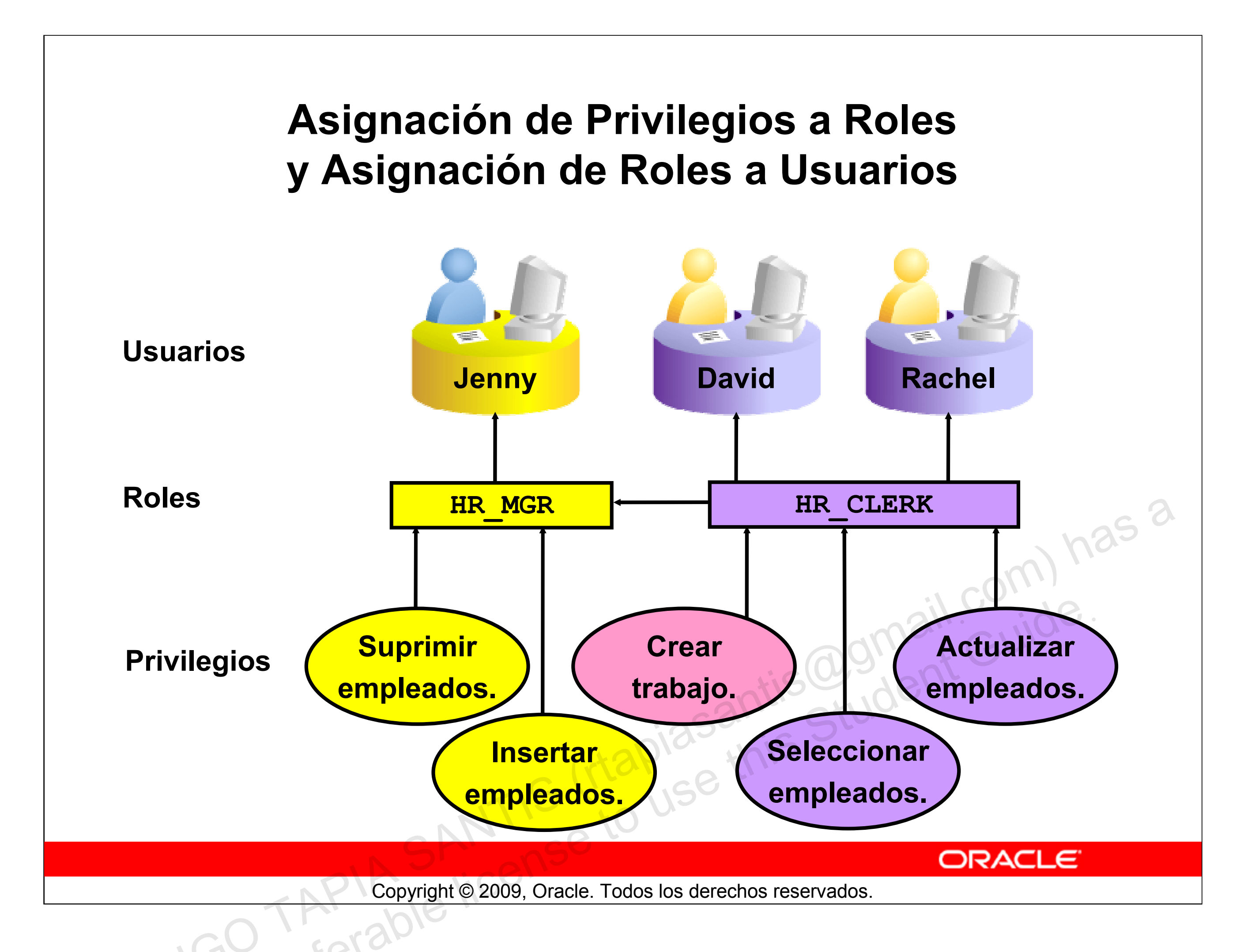
Ventajas de los Roles

- Gestión de privilegios más sencilla
- Gestión de privilegios dinámica
- Disponibilidad selectiva de privilegios



Ventajas de los Roles

- **Gestión de privilegios más sencilla:** utilice roles para simplificar la gestión de privilegios. En lugar de otorgar el mismo juego de privilegios a varios usuarios, puede otorgar los privilegios a un rol y, a continuación, otorgar dicho rol a cada usuario.
- **Gestión de privilegios dinámica:** si se modifican los privilegios asociados a un rol, todos los usuarios a los que se haya otorgado dicho rol adquieren los privilegios modificados de forma automática e inmediata.
- **Disponibilidad selectiva de privilegios:** los roles se pueden activar o desactivar para activar o desactivar privilegios temporalmente. Esto permite controlar los privilegios del usuario en una situación concreta.



Asignación de Privilegios a Roles y Asignación de Roles a Usuarios

En la mayoría de sistemas, se tarda mucho y se pueden producir errores al otorgar los privilegios necesarios a cada usuario de forma individual. El software de Oracle permite una gestión de privilegios sencilla y controlada mediante roles. Los roles son grupos con nombre de privilegios relacionados que se otorgan a los usuarios o a otros roles. Los roles están diseñados para facilitar la administración de privilegios en la base de datos y, por lo tanto, mejorar la seguridad.

Características de los Roles

- Se otorgan y revocan privilegios de los roles como si el rol fuera un usuario.
- Se otorgan y revocan roles de usuarios u otros roles como si fueran privilegios del sistema.
- Un rol puede constar de privilegios del sistema y de objeto.
- Un rol se puede activar o desactivar para cada usuario al que se le otorgue dicho rol.
- Un rol puede necesitar la activación de una contraseña.
- Los roles no son propiedad de nadie y no están en ningún esquema.

En el ejemplo de la diapositiva, los privilegios `SELECT` y `UPDATE` de la tabla `employees`, *así como* el privilegio del sistema `CREATE JOB` se otorgan al rol `HR_CLERK`. Los privilegios `DELETE` e `INSERT` de la tabla `employees`, *así como* el rol `HR_CLERK` se otorgan al rol `HR_MGR`.
Al gestor se le otorga el rol `HR_MGR`, por lo que puede seleccionar, suprimir, insertar y actualizar la tabla `employees`.

Roles Predefinidos

Rol	Privilegios Incluidos
CONNECT	CREATE SESSION
RESOURCE	CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE
SCHEDULER_ ADMIN	CREATE ANY JOB, CREATE EXTERNAL JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
DBA	Tiene la mayoría de privilegios del sistema; otros muchos roles. No otorgar a usuarios que no sean administradores.
SELECT_ CATALOG_ROLE	No tiene privilegios del sistema; HS_ADMIN_ROLE y más de 1.700 privilegios de objeto en el diccionario de datos

ORACLE

Roles Predefinidos

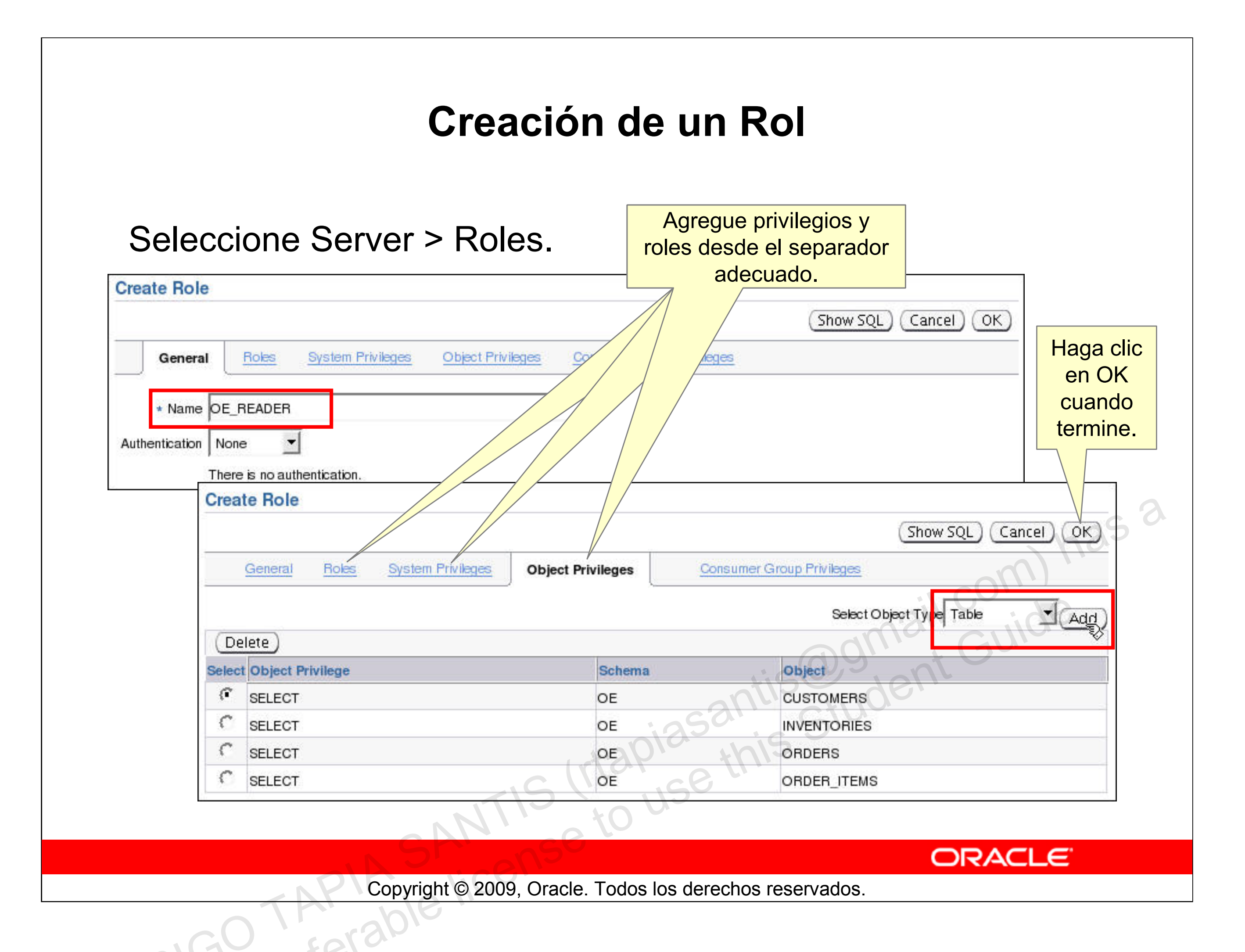
Existen varios roles definidos automáticamente para Oracle Database al ejecutar los scripts de creación de bases de datos. CONNECT se otorga automáticamente a cualquier usuario creado con Enterprise Manager. Por motivos de seguridad, el rol CONNECT sólo contiene el privilegio CREATE SESSION desde la versión 10.2.0 de Oracle Database.

Nota: tenga en cuenta que al otorgar el rol RESOURCE también se otorga el privilegio UNLIMITED TABLESPACE.

Roles Funcionales

Se crean otros roles que le autorizan a administrar funciones especiales, cuando se instala esta funcionalidad. Por ejemplo, XDBADMIN contiene los privilegios necesarios para administrar la base de datos XML (Extensible Markup Language) si esta función está instalada. AQ_ADMINISTRATOR_ROLE proporciona privilegios para administrar el servicio de gestión de colas avanzada. HS_ADMIN_ROLE incluye los privilegios necesarios para administrar servicios heterogéneos.

No debe modificar los privilegios otorgados a estos roles funcionales sin la ayuda de los Servicios de Soporte Oracle, porque podría desactivar involuntariamente la funcionalidad necesaria.



Creación de un Rol

Un *rol* es un grupo con nombre de privilegios relacionados que se otorgan a los usuarios o a otros roles. Un DBA gestiona los privilegios mediante roles.

Para crear un rol, realice los siguientes pasos:

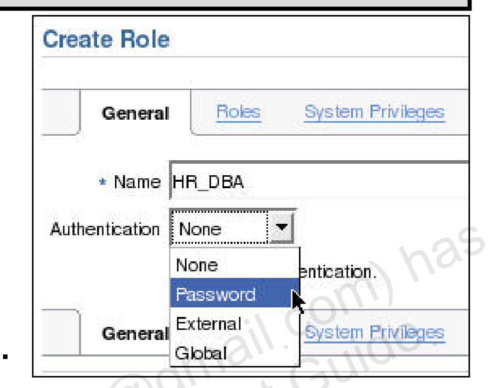
1. En Enterprise Manager Database Control, haga clic en el separador Server y, a continuación, haga clic en Roles en la cabecera Security.
2. Haga clic en el botón Create.
3. En el separador General, introduzca un nombre para el rol.
4. De manera opcional, agregue los privilegios del sistema, los privilegios de objeto y los demás roles necesarios. El rol se puede editar más adelante para modificar esta configuración si es necesario.
5. Haga clic en OK cuando termine.

Roles Seguros

- Los roles no tienen que ser por defecto, sino que se pueden activar cuando sean necesarios.

```
SET ROLE vacationdba;
```

- Los roles se pueden proteger mediante la autenticación.



- Los roles también se pueden proteger mediante programación.

```
CREATE ROLE secure_application_role
IDENTIFIED USING <nombre_procedimiento_seguridad>;
```

ORACLE

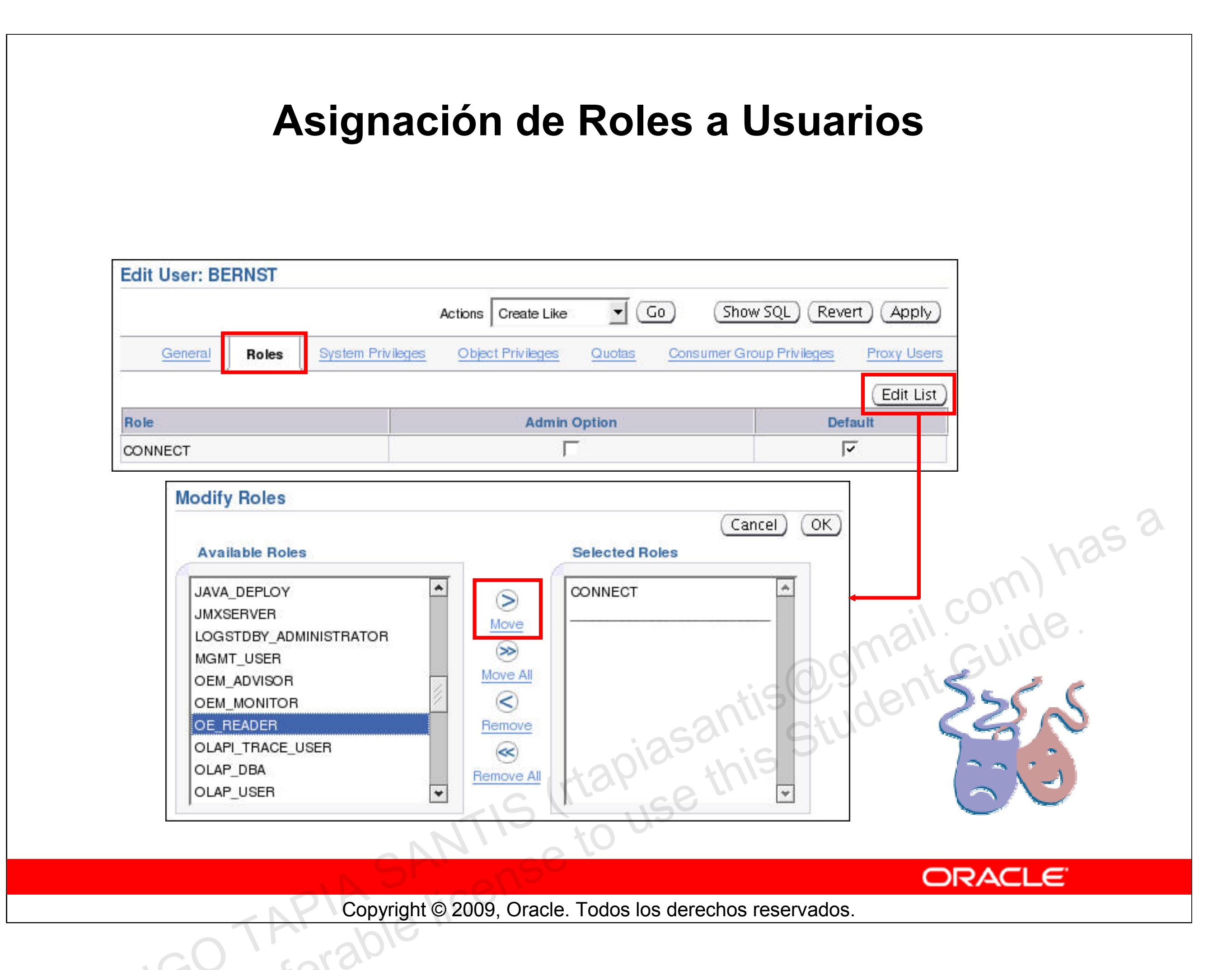
Roles Seguros

Los roles se suelen activar por defecto, lo que significa que si un rol se otorga a un usuario, dicho usuario puede ejercer los privilegios asignados al rol. Los roles por defecto se asignan al usuario en tiempo de conexión.

Es posible:

- Hacer que un rol no sea por defecto. Cuando el rol se otorga a un usuario, desactive la casilla de control DEFAULT. El usuario debe ahora activar explícitamente el rol para poder ejercer los privilegios de dicho rol.
- Exigir la autenticación adicional de un rol. La autenticación por defecto de un rol es None, pero es posible exigir la autenticación adicional del rol para poder definirlo.
- Crear roles de aplicación seguros que se puedan activar sólo mediante la ejecución correcta de un procedimiento PL/SQL. El procedimiento PL/SQL puede comprobar varias cosas como, por ejemplo, la dirección de red del usuario, el programa que está ejecutando el usuario, la hora del día y cualquier otro elemento necesario para proteger de forma adecuada un grupo de permisos.
- Administrar roles con facilidad mediante la opción de Oracle Database Vault. Se simplifican los roles de aplicaciones seguros y se pueden restringir aún más los roles tradicionales.

Asignación de Roles a Usuarios



Asignación de Roles a Usuarios

Puede utilizar los roles para administrar privilegios de base de datos. Puede agregar privilegios a un rol y otorgar dicho rol a un usuario. El usuario puede activar el rol y ejercer los privilegios otorgados por el mismo. Un rol contiene todos los privilegios otorgados a dicho rol y todos los privilegios de otros roles que se le hayan asignado.

Por defecto, Enterprise Manager otorga automáticamente el rol `CONNECT` a los usuarios nuevos. De esta forma, los usuarios se pueden conectar a la base de datos y crear objetos de base de datos en sus propios esquemas.

Para asignar un rol a un usuario:

1. En Enterprise Manager Database Control, haga clic en el separador Server y, a continuación, haga clic en Users en la cabecera Security.
2. Seleccione el usuario y haga clic en el botón Edit.
3. Haga clic en el separador Roles y, a continuación, en el botón Edit List.
4. Seleccione el rol deseado en Available Roles y muévalo hasta Selected Roles.
5. Cuando haya asignado todos los roles adecuados, haga clic en el botón OK.

Prueba

Todas las contraseñas creadas en Oracle Database 11*g* no son sensibles a mayúsculas/minúsculas por defecto.

1. Verdadero
2. Falso

ORACLE

Respuesta: 2

Prueba

Un rol de base de datos:

1. Se puede activar o desactivar
2. Puede constar de privilegios de sistema y de objeto
3. Pertenece a su creador
4. No se puede proteger con contraseña

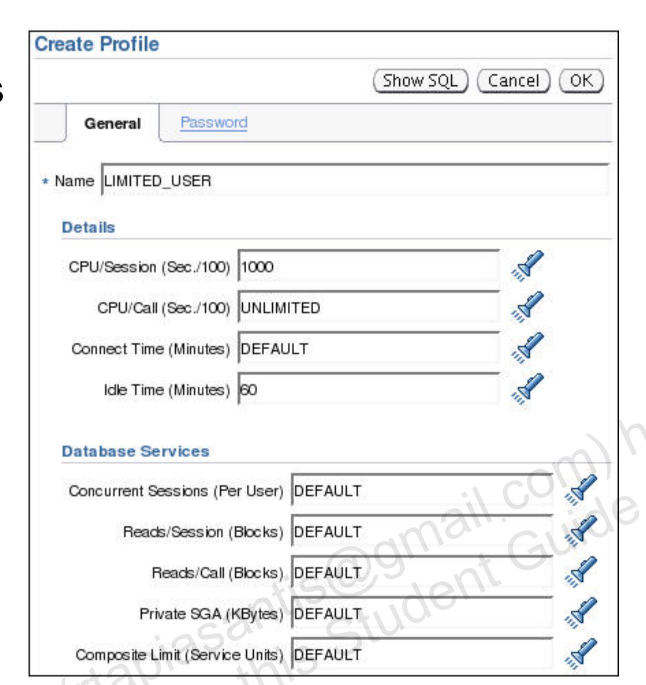
Respuestas: 1, 2

Perfiles y Usuarios

A los usuarios sólo se les asigna un perfil a la vez.

Perfiles:

- Controlan el uso de recursos
- Gestionan el estado de las cuentas y la caducidad de las contraseñas



Nota: `RESOURCE_LIMIT` se debe definir en `TRUE` para que los perfiles puedan imponer limitaciones de recursos.

ORACLE

Perfiles y Usuarios

Los perfiles imponen un juego con nombre de límites de recursos en cuanto al uso de la base de datos y de los recursos de la instancia. Los perfiles también gestionan el estado de las cuentas y establecen limitaciones en cuanto a las contraseñas de usuarios (longitud, fecha de vencimiento, etc.). Cada uno de los usuarios se asigna a un perfil y puede pertenecer sólo a un perfil en un momento determinado. Si los usuarios ya se han conectado cuando cambia su perfil, el cambio no se aplica hasta la siguiente conexión.

El perfil `DEFAULT` sirve como base para todos los demás perfiles. Como se ilustra en la diapositiva, las limitaciones para un perfil pueden estar especificadas implícitamente (como en CPU/Session), pueden ser ilimitadas (como en CPU/Call) o pueden hacer referencia a la configuración del perfil `DEFAULT` (como en Connect Time).

Los perfiles no pueden imponer limitaciones de recursos a los usuarios, a menos que el parámetro de inicialización `RESOURCE_LIMIT` esté definido en `TRUE`. Si `RESOURCE_LIMIT` tiene su valor por defecto `FALSE`, se ignoran las limitaciones de recursos del perfil. Siempre se aplica la configuración de contraseña de los perfiles.

Los perfiles permiten al administrador controlar los siguientes recursos del sistema:

- **CPU:** los recursos de CPU pueden estar limitados por sesión o por llamada. Una limitación de CPU/Session de 1.000 significa que si una sesión concreta que utiliza este perfil usa más de 10 segundos de tiempo de CPU (las limitaciones de tiempo de CPU se miden en centésimas de segundo), dicha sesión recibe un error y se desconecta:

```
ORA-02392: exceeded session limit on CPU usage, you are being
logged off
```

Perfiles y Usuarios (continuación)

Una limitación por llamada tiene el mismo efecto, pero en lugar de limitar la sesión general del usuario, evita que cualquier comando individual utilice demasiada CPU. Si CPU/Call está limitada y el usuario supera la limitación, se abortará el comando. El usuario recibirá un mensaje de error como el siguiente:

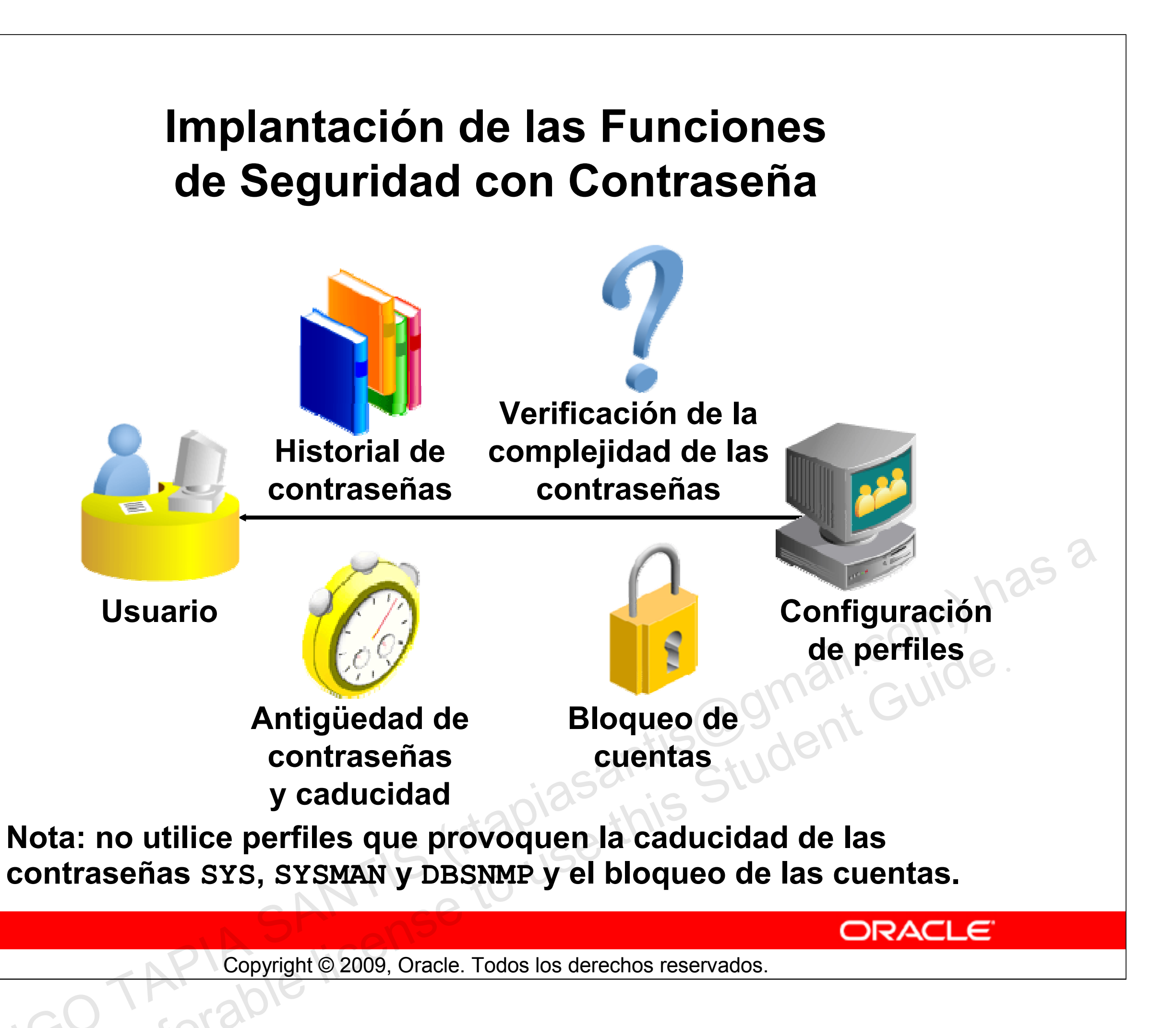
```
ORA-02393: exceeded call limit on CPU usage
```

- **Red/Memoria:** cada sesión de base de datos usa recursos de memoria del sistema y (si la sesión es desde un usuario no local al servidor) recursos de red. Puede especificar lo siguiente:
  - **Connect Time:** indica cuántos minutos puede estar conectado un usuario antes de que se le desconecte automáticamente.
  - **Idle Time:** indica cuántos minutos puede permanecer inactiva la sesión de un usuario antes de que se le desconecte automáticamente. El tiempo de inactividad se calcula sólo para el proceso de servidor. No tiene en cuenta la actividad de la aplicación. El límite `IDLE_TIME` no se ve afectado por consultas de larga duración ni otras operaciones.
  - **Concurrent Sessions:** indica cuántas sesiones simultáneas se pueden crear mediante una cuenta de usuario de base de datos
  - **Private SGA:** limita la cantidad de espacio usado en el Área Global del Sistema (SGA) para ordenación, fusión de bitmaps, etc. Esta restricción sólo tiene efecto si la sesión utiliza un servidor compartido. (Los servidores compartidos se tratan en la lección titulada "Configuración del Entorno de Red de Oracle".)
- **E/S de disco:** limita la cantidad de datos que un usuario puede leer en el nivel de sesión o en el nivel de llamada. Reads/Session y Reads/Call ponen una limitación en el número total de lecturas de la memoria y del disco. Esto se puede llevar a cabo para asegurarse de que ninguna sentencia que genere mucha E/S utilice demasiada memoria o discos.

Los perfiles también permiten un límite compuesto. Los límites compuestos se basan en una combinación ponderada de CPU/Session, Reads/Session, Connect Time y Private SGA. Los límites compuestos se tratan más detalladamente en *Oracle Database Security Guide* (Guía de Seguridad de Oracle Database).

Para crear un perfil, haga clic en el separador Server y, a continuación, haga clic en Profiles en la cabecera Security. En la página Profiles, haga clic en el botón Create.

Nota: el Gestor de Recursos es una alternativa para muchos de los valores de configuración de perfil. Para obtener más información sobre el Gestor de Recursos, consulte *Oracle Database Administrator's Guide* (Guía del Administrador de Oracle Database).



Implantación de las Funciones de Seguridad con Contraseña

La gestión de contraseñas de Oracle se implanta con perfiles de usuario. Los perfiles pueden proporcionar varias funciones estándar de seguridad.

Bloqueo de cuentas: permite el bloqueo automático de cuentas durante un período definido cuando los usuarios no han podido conectarse al sistema en el número especificado de intentos.

- **`FAILED_LOGIN_ATTEMPTS`:** especifica el número de intentos fallidos de conexión antes del bloqueo de la cuenta
- **`PASSWORD_LOCK_TIME`:** especifica el número de días que se bloqueará la cuenta tras un número concreto de intentos fallidos de conexión

Antigüedad y vencimiento de contraseñas: permite a las contraseñas de usuario tener una duración concreta, tras la cual vencen y se deben cambiar.

- **`PASSWORD_LIFE_TIME`:** determina la duración de la contraseña en días, tras la que caducará la contraseña
- **`PASSWORD_GRACE_TIME`:** especifica un período de gracia en días para cambiar la contraseña tras la primera conexión correcta después de que haya caducado la contraseña

Nota: la caducidad de las contraseñas y el bloqueo de las cuentas `SYS`, `SYSMAN` y `DBSNMP` impiden que Enterprise Manager funcione adecuadamente. Las aplicaciones deben detectar el mensaje de advertencia de contraseña vencida y manejar el cambio de contraseña. De lo contrario, el período de gracia vence y se bloquea el usuario sin que este sepa la razón.

Implantación de las Funciones de Seguridad con Contraseña (continuación)

Historial de contraseñas: comprueba la nueva contraseña para garantizar que ésta no se vuelve a utilizar durante un período especificado o un número concreto de cambios de contraseña. Estas comprobaciones se pueden implantar de una de las siguientes formas:

- **PASSWORD_REUSE_TIME:** especifica que un usuario no puede volver a utilizar una contraseña durante un número de días determinado
- **PASSWORD_REUSE_MAX:** especifica el número de cambios de contraseña necesarios antes de que se pueda volver a utilizar la contraseña actual

Recuerde que los valores de los parámetros de los perfiles se definen o se heredan del perfil `DEFAULT`.

Si ambos parámetros del historial de contraseñas tienen el valor `UNLIMITED`, Oracle Database ignora los dos. El usuario puede reutilizar cualquier contraseña en cualquier momento, lo que no es una buena práctica de seguridad.

Si se definen ambos parámetros, se permite la reutilización de contraseñas, pero sólo si se cumplen ambas condiciones. El usuario debe haber cambiado la contraseña el número de veces especificado y debe haber transcurrido el número de días especificado desde el último uso de la contraseña antigua.

Por ejemplo, el perfil del usuario `ALFRED` tiene `PASSWORD_REUSE_MAX` definido en 10 y `PASSWORD_REUSE_TIME` en 30. El usuario `ALFRED` no puede reutilizar una contraseña hasta que haya restablecido la contraseña 10 veces y hasta que hayan transcurrido 30 días desde el último uso de la contraseña.

Si un parámetro está definido en un número y el otro parámetro se ha especificado como `UNLIMITED`, el usuario nunca puede reutilizar la contraseña.

Verificación de la complejidad de las contraseñas: realiza una comprobación de la complejidad de la contraseña para verificar que cumple determinadas reglas. La comprobación se debe asegurar de que la contraseña es lo suficientemente compleja para proporcionar protección contra intrusos que puedan intentar entrar en el sistema adivinando la contraseña.

El parámetro `PASSWORD_VERIFY_FUNCTION` asigna una función PL/SQL que realiza una comprobación de la complejidad de las contraseñas antes de asignar una. Las funciones de verificación de contraseñas deben ser propiedad del usuario `SYS` y deben devolver un valor booleano (`TRUE` o `FALSE`). Se proporciona una función modelo de verificación de contraseñas en el script `utlpwdmg.sql`, que está en los siguientes directorios:

- Plataformas Unix y Linux: `$ORACLE_HOME/rdbms/admin`
- Plataformas Windows: `%ORACLE_HOME%\rdbms\admin`

Creación de un Perfil de Contraseña

Create Profile

Show SQL | Cancel | OK

General | Password

Password

Expire in (days): 90

Lock (days past expiration): 10

History

Number of passwords to keep: 2

Number of days to keep for: UNLIMITED

Complexity

Complexity function: VERIFY_FUNCTION_11G

Failed Login

Number of failed login attempts to lock after: 3

Number of days to lock for: 5/1440

ORACLE

Creación de un Perfil de Contraseña

Para crear un perfil de contraseña, haga clic en el separador Server y, a continuación, haga clic en Profiles en la cabecera Security. En la página Profiles, haga clic en el botón Create. Haga clic en el separador Password para definir los límites de la contraseña.

Se pueden seleccionar de una lista los valores comunes para cada una de las opciones (haga clic en el icono de linterna para examinar) o bien puede introducir un valor personalizado.

Todos los períodos de tiempo están expresados en días, pero también se pueden expresar como fracciones. Hay 1.440 minutos en un día, por lo que 5/1.440 son cinco minutos.

Enterprise Manager también se puede utilizar para editar perfiles de contraseña existentes.

Si se ha ejecutado el script `utlpwdmg.sql`, están disponibles las funciones `VERIFY_FUNCTION` y `VERIFY_FUNCTION_11G`. Si ha creado su propia función de complejidad, puede introducir el nombre de dicha función. El nombre de la función no aparece en la lista Select. Si la función produce errores de tiempo de ejecución, el usuario no puede cambiar la contraseña.

Borrado de un Perfil de Contraseña

En Enterprise Manager, no se puede borrar un perfil utilizado por usuarios. Sin embargo, si borra un perfil con la opción `CASCADE` (en SQL*Plus, por ejemplo), a todos los usuarios con ese perfil se les asigna de forma automática el perfil `DEFAULT`.

Función de Verificación de Contraseñas Proporcionada: **VERIFY_FUNCTION_11G**

La función VERIFY_FUNCTION_11G garantiza que la contraseña:

- Tiene al menos ocho caracteres
- Es diferente del nombre de usuario, del nombre de usuario con un número o del nombre de usuario invertido
- Es diferente del nombre de la base de datos o del nombre de la base de datos con un número
- Es una cadena con al menos un carácter alfabético y uno numérico
- Es diferente de la contraseña anterior en al menos tres letras

Consejo: utilice esta función como plantilla para crear su propia verificación de contraseñas personalizada.

ORACLE

Función de Verificación de Contraseñas Proporcionada: **VERIFY_FUNCTION_11G**

El servidor de Oracle proporciona dos funciones de verificación de la complejidad de las contraseñas denominadas VERIFY_FUNCTION y VERIFY_FUNCTION_11g. Estas funciones se crean con el script <oracle_home>/rdbms/admin/utlpwdmg.sql. VERIFY_FUNCTION se proporciona para quienes prefieren la función de contraseña proporcionada con versiones anteriores. La función de verificación de la complejidad de las contraseñas se debe crear en el esquema SYS. Se puede utilizar como plantilla para su verificación de contraseñas personalizada.

Además de crear VERIFY_FUNCTION, el script utlpwdmg también cambia el perfil DEFAULT con el siguiente comando ALTER PROFILE:

```
ALTER PROFILE default LIMIT
PASSWORD_LIFE_TIME 180
PASSWORD_GRACE_TIME 7
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX UNLIMITED
FAILED_LOGIN_ATTEMPTS 10
PASSWORD_LOCK_TIME 1
PASSWORD_VERIFY_FUNCTION verify_function_11g;
```

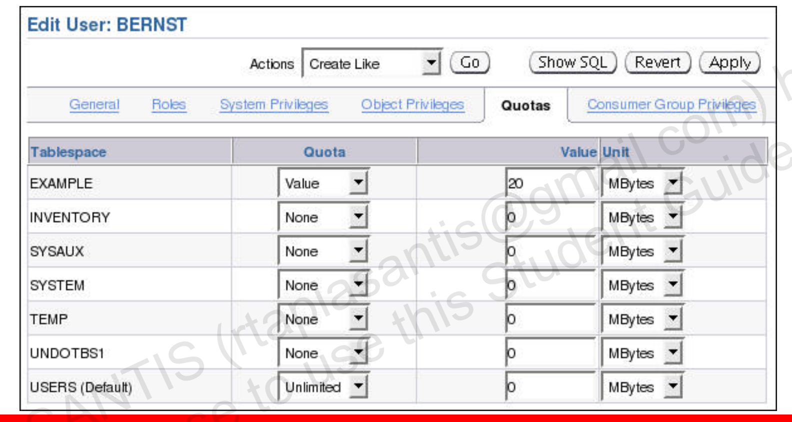
Recuerde que cuando se crean usuarios, se les asigna el perfil DEFAULT, a menos que se especifique otro.

Asignación de Cuotas a Usuarios

Se debe asignar una cuota a los usuarios que no tienen el privilegio del sistema `UNLIMITED TABLESPACE` para que puedan crear objetos en un tablespace.

Las cuotas pueden ser:

- Un valor concreto en megabytes o kilobytes
- Ilimitadas



Asignación de Cuotas a Usuarios

La *cuota* es un espacio asignado en un tablespace determinado. Por defecto, un usuario no tiene ninguna cuota en ningún tablespace. Dispone de tres opciones para proporcionar una cuota a un usuario en un tablespace.

- **Unlimited:** permite al usuario utilizar todo el espacio disponible en el tablespace.
- **Value:** es el número de kilobytes o megabytes que el usuario puede utilizar. Esto no garantiza que el espacio se reserve para el usuario. Este valor puede ser mayor o menor que el espacio actual disponible en el tablespace.
- Privilegio del sistema **`UNLIMITED TABLESPACE`:** sustituye a todas las cuotas de tablespace individuales y proporciona al usuario una cuota ilimitada en todos los tablespaces, incluidos `SYSTEM` y `SYSAUX`. Este privilegio se debe otorgar con cautela.
  Nota: tenga en cuenta que al otorgar el rol `RESOURCE`, también se otorga este privilegio.

No debe proporcionar cuota a los usuarios en los tablespaces `SYSTEM` o `SYSAUX`. Normalmente, sólo los usuarios `SYS` y `SYSTEM` pueden crear objetos en los tablespaces `SYSTEM` o `SYSAUX`.

No necesita ninguna cuota en un tablespace temporal asignado ni en ningún tablespace de deshacer. No necesita ninguna cuota para poder insertar, actualizar y suprimir datos en Oracle Database. Los únicos usuarios que necesitan una cuota son las cuentas que poseen los objetos de la base de datos. Al instalar código de aplicaciones, es normal que Installer cree cuentas de base de datos a las que pertenezcan los objetos. Sólo estas cuentas necesitan una cuota. Se puede otorgar permiso a otros usuarios de la base de datos para que utilicen estos objetos sin necesidad de cuota alguna.

Asignación de Cuotas a Usuarios (continuación)

- La instancia de Oracle comprueba la cuota cuando un usuario crea o amplía un segmento.
- En el caso de las actividades asignadas a un esquema de usuario, sólo cuentan para la cuota las actividades que utilizan espacio de un tablespace. Las actividades que no utilizan espacio en el tablespace asignado no afectan a la cuota (como la creación de vistas o el uso de tablespaces temporales).
- La cuota se repone cuando los objetos propiedad del usuario se borran con la cláusula `PURGE` o cuando los objetos propiedad del usuario de la papelera de reciclaje se depuran.

Aplicación del Principio de Privilegio Más Bajo

- Protección del diccionario de datos:

```
O7_DICTIONARY_ACCESSIBILITY=FALSE
```

- Revocación de privilegios innecesarios de PUBLIC.
- Uso de listas de control de acceso (ACL) para controlar el acceso a la red.
- Restricción de los directorios a los que pueden acceder los usuarios.
- Limitación de usuarios con privilegios administrativos.
- Restricción de la autenticación de la base de datos remota:

```
REMOTE_OS_AUTHENT=FALSE
```


ORACLE

Aplicación del Principio de Privilegio Más Bajo

El principio de privilegio más bajo significa que se debe dar a un usuario sólo aquellos privilegios que sean necesarios para realizar de forma eficaz una tarea. De esta forma se reducen las posibilidades de que los usuarios modifiquen o visualicen los datos (tanto de forma accidental como no autorizada) para los que no tienen privilegios de modificación o visualización.

Protección del diccionario de datos: el parámetro O7_DICTIONARY_ACCESSIBILITY se define por defecto en FALSE. No permita que se cambie este valor sin un buen motivo, ya que impide a los usuarios con privilegios del sistema ANY TABLE acceder a las tablas base del diccionario de datos. También garantiza que el usuario SYS se puede conectar sólo como SYSDBA.

Revocación de privilegios innecesarios de PUBLIC: hay varios paquetes que son muy útiles para aplicaciones que los necesitan, pero requieren una configuración correcta para utilizarlos de forma segura. A PUBLIC se le otorga el privilegio de ejecución en los siguientes paquetes: UTL_SMTP, UTL_TCP, UTL_HTTP y UTL_FILE. En Oracle Database 11*g*, el acceso a la red está controlado por una lista de control de acceso (ACL) que se puede configurar para permitir que ciertos usuarios accedan a servicios de red concretos. El acceso a la red se deniega por defecto. Se debe crear una ACL para permitir el acceso a la red. El acceso a archivos mediante UTL_FILE se controla en dos niveles: a nivel del sistema operativo, con permisos para archivos y directorios y, en la base de datos, mediante objetos DIRECTORY que permiten el acceso a directorios concretos del sistema de archivos. El objeto DIRECTORY se puede otorgar a un usuario para lectura o para lectura y escritura. Se deben controlar con cuidado los privilegios de ejecución para otros paquetes PL/SQL.

Aplicación del Principio de Privilegio Más Bajo (continuación)

Entre los paquetes más potentes que se podrían utilizar de forma incorrecta se incluyen:

- **`UTL_SMTP`:** permite que se envíen mensajes de correo electrónico arbitrarios mediante el uso de la base de datos como servidor de correo de Protocolo Simple de Transferencia de Correo (SMTP). Utilice la ACL para controlar a qué máquinas puede acceder cada usuario.
- **`UTL_TCP`:** permite al servidor de base de datos establecer conexiones de red salientes con cualquier servicio de red de recepción o en espera. Por lo tanto, se pueden enviar datos arbitrarios entre el servidor de base de datos y cualquier servido de red en espera. Utilice la ACL para controlar el acceso.
- **`UTL_HTTP`:** permite al servidor de base de datos solicitar y recuperar datos a través de HTTP. Al otorgar este paquete a un usuario, se puede permitir el envío de datos a través de pantallas HTML a sitios web no autorizados. Limite el acceso con la ACL.
- **`UTL_FILE`:** si se configura incorrectamente, permite el acceso de nivel de texto a cualquier archivo del sistema operativo de host. Si se configura correctamente, este paquete limita el acceso de los usuarios a determinadas ubicaciones de directorio.

Restricción de acceso a directorios del sistema operativo: el objeto `DIRECTORY` de la base de datos permite a los DBA asignar directorios a rutas de acceso del sistema operativo y otorgar privilegios sobre esos directorios a usuarios individuales.

Limitación de usuarios con privilegios administrativos: no proporcione a los usuarios de base de datos más privilegios de los necesarios. No otorgue el rol DBA a usuarios que no sean administradores. Para implantar el privilegio más bajo, restrinja los siguientes tipos de privilegios:

- Otorgamientos de privilegios de sistema y de objeto
- Conexiones a la base de datos con privilegios `SYS`, como `SYSDBA` y `SYSOPER`
- Otros privilegios de tipo DBA, como `DROP ANY TABLE`

Restricción de la autenticación de la base de datos remota: el parámetro `REMOTE_OS_AUTHENT` se define en `FALSE` por defecto. No se debe cambiar, a menos que se pueda confiar en todos los clientes para autenticar de manera adecuada a los usuarios. Con la llegada del almacén seguro y externo de contraseñas (disponible en Oracle Database 10*g* versión 2), existen pocos motivos de peso para permitir la autenticación del sistema operativo remota.

En el proceso de autenticación remota:

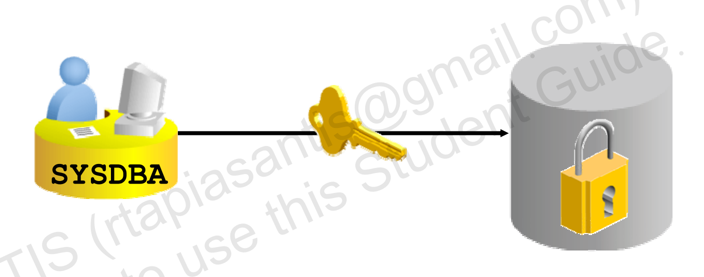
- El usuario de base de datos se autentica de forma externa
- El sistema remoto autentica el usuario
- El usuario se conecta a la base de datos sin ninguna otra autenticación

Nota: someta sus aplicaciones siempre a pruebas exhaustivas si ha revocado privilegios.

Protección de Cuentas con Privilegios

Las cuentas con privilegios se pueden proteger:

- Utilizando el archivo de contraseñas con contraseñas sensibles a mayúsculas/minúsculas
- Activando una autenticación compleja para los roles de administrador



Definición de la Autenticación de Administrador de Base de Datos

Los usuarios con privilegios SYSDBA, SYSOPER o SYSASM se deben autenticar siempre. Al realizar una conexión local, el sistema operativo local autentica al usuario si es miembro de un grupo del sistema operativo con privilegios. Si se realiza una conexión remota, se utiliza un archivo de contraseñas para autenticar a los usuarios con privilegios. Si el archivo de contraseñas está configurado, primero se comprobará. En Oracle Database 11*g*, estas contraseñas son sensibles a mayúsculas/minúsculas. Oracle Database 11*g* proporciona otros métodos para hacer que la autenticación remota del administrador sea más segura y centralizar la administración de estos usuarios con privilegios.

Cuando se crea una base de datos con el Asistente de Configuración de Bases de Datos, el archivo de contraseñas es sensible a mayúsculas/minúsculas. Si actualiza versiones anteriores de la base de datos, asegúrese de que el archivo de contraseñas sea sensible a mayúsculas/minúsculas para las conexiones remotas:

```
orapwd file=orapworcl entries=5 ignorecase=N
```

Si la preocupación reside en que el archivo de contraseñas sea vulnerable o que el mantenimiento de muchos archivos de contraseñas sea una carga, se puede implantar la autenticación compleja. Necesita Advanced Security Option si desea utilizar métodos de autenticación compleja. Para obtener más información sobre la autenticación compleja, consulte la guía *Oracle Database Advanced Security Administrator's Guide* (Guía del Administrador de Seguridad Avanzada de Oracle Database).

Prueba

La aplicación del principio de privilegio más bajo no es suficiente para reforzar Oracle Database.

1. Verdadero
2. Falso

ORACLE

Respuesta: 1

Prueba

Si RESOURCE_LIMIT está definido en su valor por defecto FALSE, se ignoran las limitaciones de contraseñas del perfil.

1. Verdadero
2. Falso

ORACLE

Respuesta: 2

Resumen

En esta lección, debe haber aprendido lo siguiente:

- Crear y gestionar cuentas de usuario de base de datos:
  - Autenticar usuarios
  - Asignar áreas de almacenamiento por defecto (tablespaces)
- Otorgar y revocar privilegios
- Crear y gestionar roles
- Crear y gestionar perfiles:
  - Implantar funciones estándar de seguridad con contraseña
  - Controlar el uso de recursos por los usuarios

ORACLE

Visión General de la Práctica 8: Administración de Usuarios

En esta práctica se abordan los siguientes temas:

- Creación de un perfil para limitar el uso de recursos
- Creación de dos roles:
  - `HRCLERK`
  - `HRMANAGER`
- Creación de cuatro usuarios nuevos:
  - Un superior y dos oficinistas
  - Un usuario de esquema para la próxima sesión práctica

ORACLE